TSI
Technical Security
& Intelligence

Computer Forensics: Overview

By John Daniele

President and CEO

Technical Security & Intelligence Inc.
http://www.tsintel.com

Strategy Clarity Trust

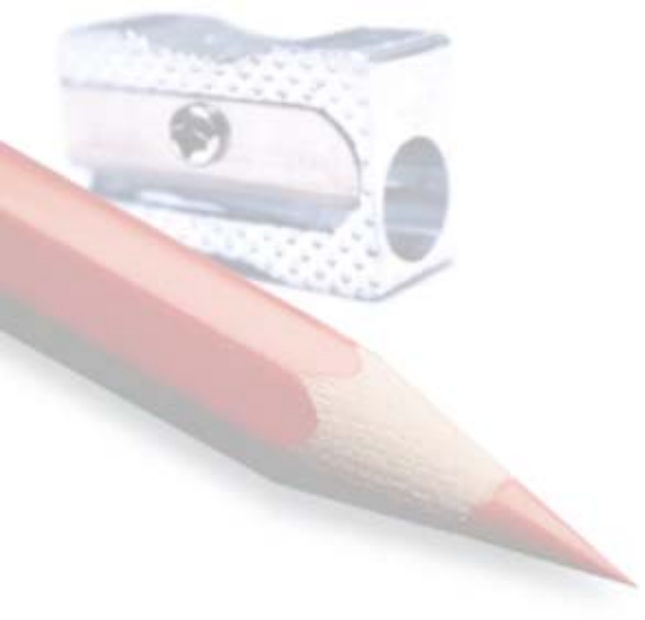
What is Computer Forensics?

TSI
Technical Security
& Intelligence

- Definition:

"Computer Forensics is the collection of techniques, processes and procedures used to preserve, extract, analyze and present electronic evidence within criminal or civil court."

Therefore, these techniques, processes and procedures must be executed in accordance with the evidentiary rules and standards of the law.



What is Computer Forensics?

TSI
Technical Security & Intelligence

- I am a Company, why does this apply to me?

- 97% of our cases have resulted in civil or criminal litigation (36/37 cases in '03)

-OPP Correctional Investigation Services Unit (CISU) document in their annual report that 49% of cases in 2002 pertained to employee misconduct

Following a forensically sound process will:

-Ensure that if evidence of a crime is encountered, the steps taken will not invalidate any ensuing police investigation if required

-Leaves your legal options open (recouping damages in civil court)

-Avoid wrongful dismissal or Union lawsuits

What is Computer Forensics?

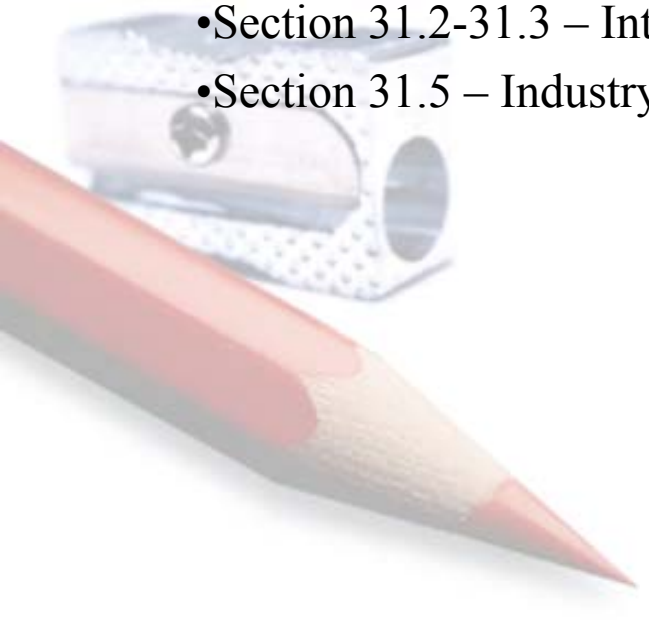
TSI
Technical Security & Intelligence

Canada Evidence Act:

Establishes rules and standards that must be met in order for evidence to be deemed admissible in court.

The rules governing the admissibility of electronic records are as follows;

- Section 31.1 – Authentication of Electronic Record
- Section 31.2-31.3 – Integrity of Electronic Record
- Section 31.5 – Industry "Best Practices"



What is Computer Forensics?

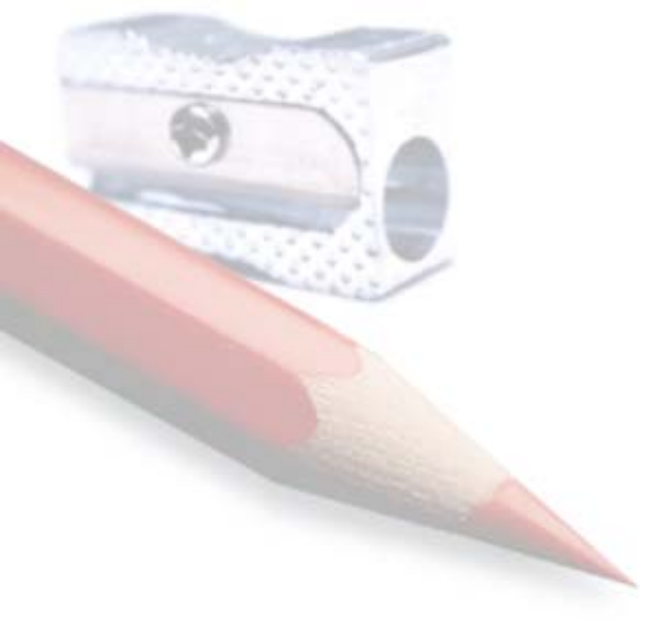
TSI
Technical Security
& Intelligence

- Canada Evidence Act:

Section 31.1 – Authentication of Electronic Evidence

-Burden of proof of authenticity lies with the person seeking to admit

-Must provide other evidence to support the evidence's authenticity



What is Computer Forensics?

TSI
Technical Security & Intelligence

- Canada Evidence Act:

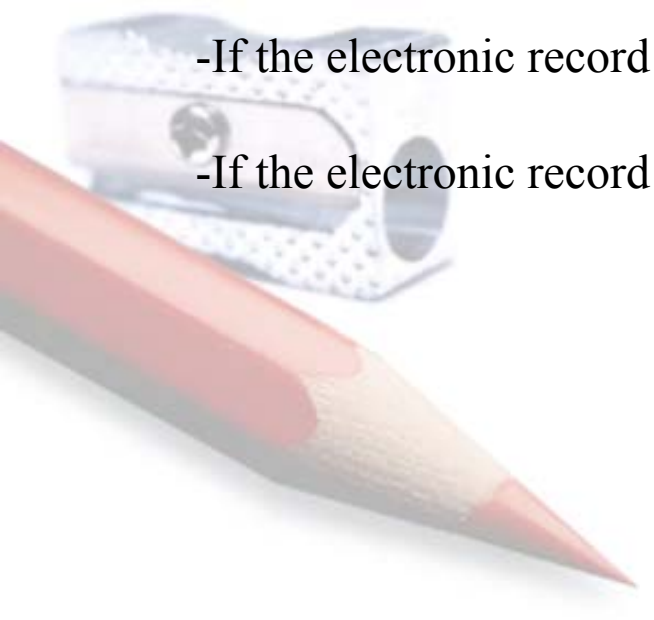
Section 31.2 – Integrity of Electronic Record

Rule of "Best Evidence" satisfied:

-If proof of the integrity of the system that generated, recorded or stored the electronic evidence is presented.

-If the electronic record is signed by secure electronic signature

-If the electronic record is printed and consistently acted or relied upon



What is Computer Forensics?

TSI
Technical Security & Intelligence

- Canada Evidence Act:

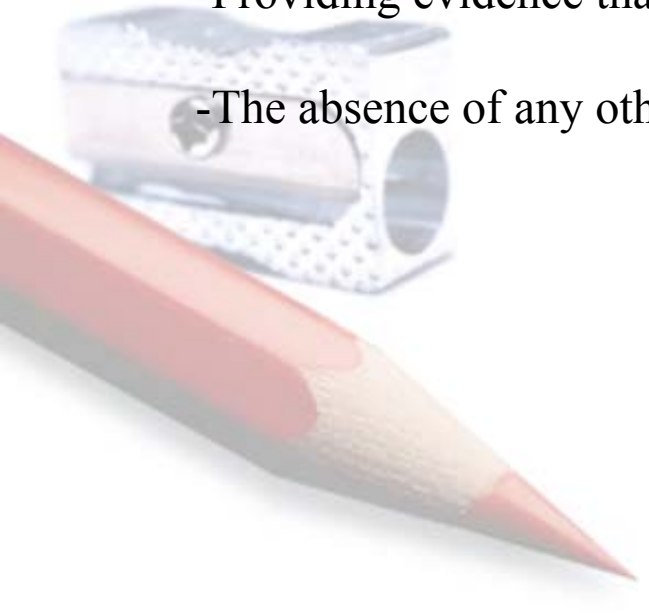
Section 31.3 – Integrity of Electronic Record

In the absence of information to the contrary, system integrity is proven by:

-Providing evidence that the system time is correct

-Providing evidence that the system is operating properly

-The absence of any other reasonable doubt



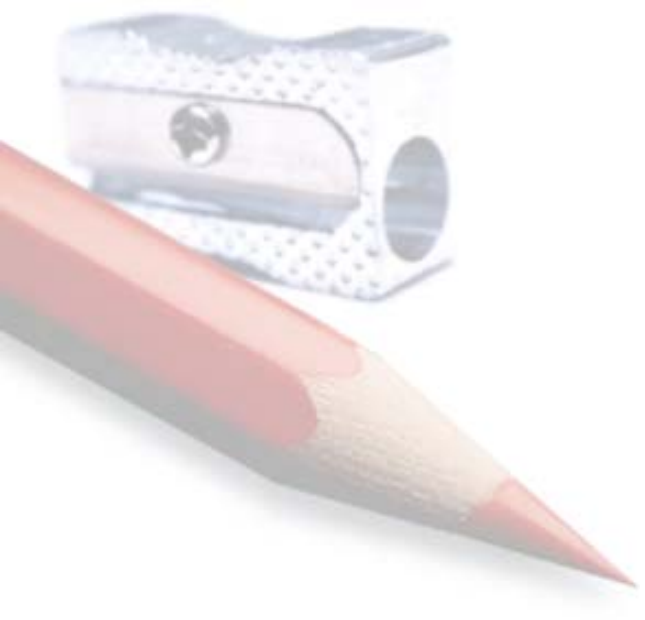
What is Computer Forensics?

TSI
Technical Security & Intelligence

- Canada Evidence Act:

Section 31.5 – Industry "Best Practices"

The courts are allowed to take into consideration generally accepted practices or procedures pertaining to the recording or storage of electronic records when determining the admissibility of evidence.



What is Computer Forensics?

TSI
Technical Security
& Intelligence

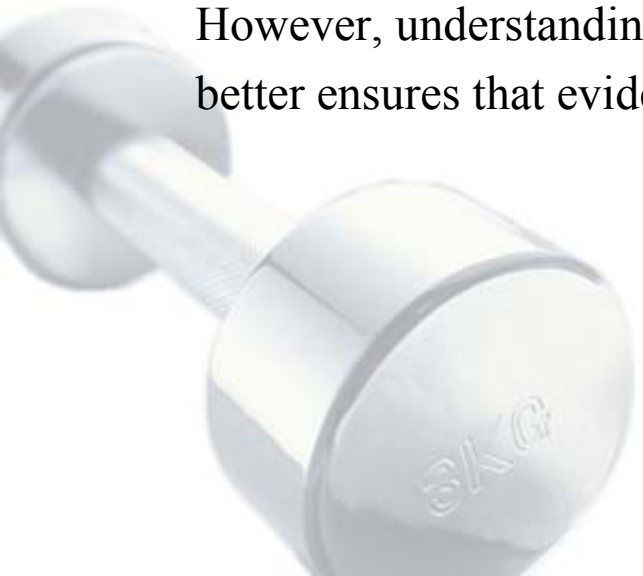
▪ Admissibility Challenge

The challenge posed by the Evidence Act is not easily overcome because electronic records are by nature:

-Extremely volatile

-Highly susceptible to tampering

However, understanding and applying the basic tenets of Computer Forensics better ensures that evidence will be admissible.



Meeting the Challenge

TSI
Technical Security
& Intelligence

4 Cardinal Rules of Evidence

1) **NEVER** mishandle evidence.

2) **NEVER** trust the subject operating system or machine

3) **NEVER** work on the original evidence

4) **DOCUMENT EVERYTHING!**

James Holley

Violating any one of these rules will invalidate your evidence. However, so long as these rules are kept, the specific processes and procedures used may be tailored to your unique circumstances.

Meeting the Challenge

TSI
Technical Security
& Intelligence

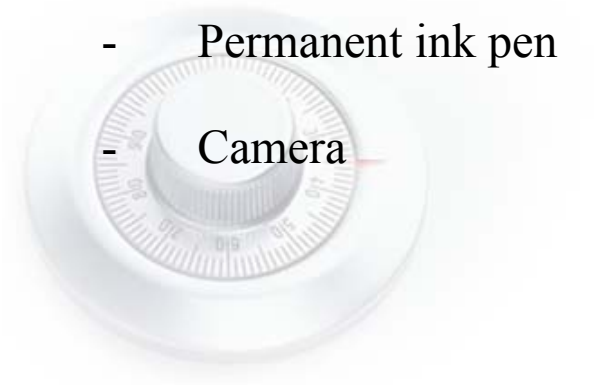
▪ Rule #1 – NEVER mishandle evidence

When obtaining or receiving evidence it is important to handle and process it in a manner which preserves its integrity.

Step 1: Establish and maintain 'Chain of Custody'

Tools required:

- Evidence notebook
- Tamper evident labels (sticky labels will do)
- Permanent ink pen
- Camera



Meeting the Challenge

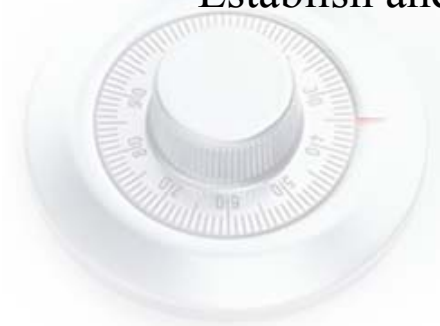
TSI
Technical Security
& Intelligence

▪ Rule #1 – NEVER mishandle evidence

Step 1: Establish and maintain 'Chain of Custody

Document the following:

- Who reported the incident along with critical date and times
- Details leading up to formal investigation
- Names of all people conducting investigation
- Establish and maintain detailed 'activity log'



Meeting the Challenge

TSI
Technical Security & Intelligence

- **Rule #1 – NEVER mishandle evidence**

Step 1: Establish and maintain 'Chain of Custody'

- Take pictures of the evidence
- Document 'crime scene' details
- Document identifiable markings on evidence

Meeting the Challenge

TSI
Technical Security
& Intelligence

- **Rule #1 – NEVER mishandle evidence**

Step 1: Establish and maintain 'Chain of Custody

- Catalog the system contents
- Document serial numbers, model numbers, asset tags

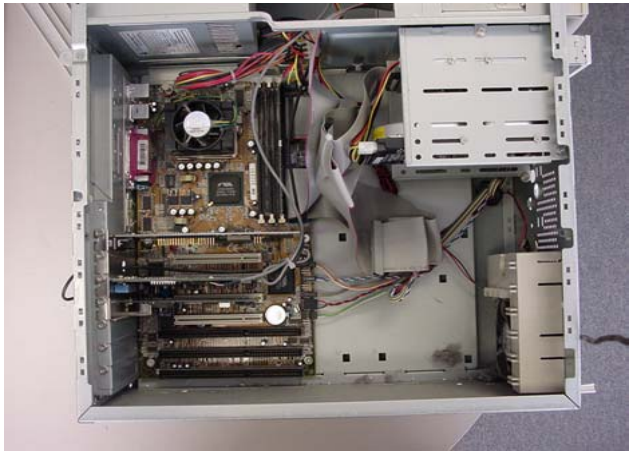
Meeting the Challenge

TSI
Technical Security
& Intelligence

- **Rule #1 – NEVER mishandle evidence**

Step 1: Establish and maintain 'Chain of Custody

- Catalog the system contents
- Document serial numbers, model numbers, asset tags



Meeting the Challenge

TSI
Technical Security
& Intelligence

▪ Rule #1 – NEVER mishandle evidence

Step 1: Establish and maintain 'Chain of Custody

- Catalog the system contents
- Document serial numbers, model numbers, asset tags

Meeting the Challenge

TSI
Technical Security
& Intelligence

- **Rule #1 – NEVER mishandle evidence**

Step 1: Establish and maintain 'Chain of Custody

- Catalog the system contents
- Document serial numbers, model numbers, asset tags

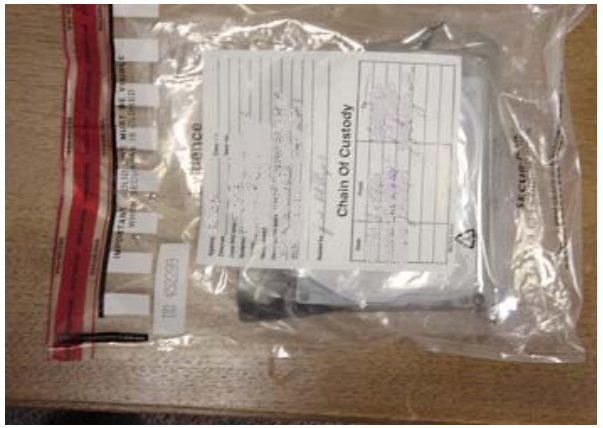
Meeting the Challenge

TSI
Technical Security & Intelligence

- **Rule #1 – NEVER mishandle evidence**

Step 1: Establish and maintain 'Chain of Custody

- "Bag" it!
- Maintain Chain Of Custody on tamperproof evidence bag
- Take a picture!



TSI Technical Security & Intelligence

Rule #2 – NEVER trust the subject OS or machine

Step 2: Forensic Imaging

- Never image a system using the subject machine!
- Always use a trusted machine that has been tested and proven to be reliable
- "Live" Forensics should be avoided unless:
  - There is good reason to believe there is volatile information of value
  - There is good reason to believe that usable information would be lost upon shutdown (drive encryption)
  - Suspect is actively using the machine at time of Search & Seizure

TSI
Technical Security & Intelligence

Rule #3 – NEVER work on original evidence

Step 2: Forensic Imaging

- Avoid accessing the file system during imaging (Use safe boot disk)
- Obtain bitstream copy of entire **physical drive** (EnCase, Safeback, 'dd')
- Document any errors detected during imaging process (bad sectors)

TSI
Technical Security & Intelligence

Rule #4 – Document Everything!

Components of Forensics Report:

- **Executive Summary**. Detail the facts established about the incident in simple, easy to understand terms.
- **Detailed Activity Log.** What was done? Where was it done? When?
- **Proof of Process Photos**
- **Forensic Imaging Process**
- **Restoration and Verification of Images**
- **Document evidence discovered during analysis**

Case Closed

TSI
Technical Security
& Intelligence

John Daniele

johnd@tsintel.com

(416) 684-3627